

**ADVERTISING SELF-REGULATORY COUNCIL/COUNCIL OF BETTER  
BUSINESS BUREAUS**

***ONLINE INTEREST-BASED ADVERTISING ACCOUNTABILITY PROGRAM***

**FORMAL REVIEW**  
Case Number: 64-2016

COMPANY: )  
iTriage LLC )  
 )  
 )  
CHALLENGER: )  
Online Interest-Based )  
Advertising Accountability Program )  
 )  
 )

**DECISION**

DATE: July 14, 2016

**SYNOPSIS**

The Digital Advertising Alliance’s (DAA) Self-Regulatory Principles (DAA Principles)<sup>1</sup> cover entities engaged in interest-based advertising (IBA) across websites and mobile applications (apps). Mobile app publishers<sup>2</sup> that authorize third parties to collect data through their apps must comply with DAA Principles. In particular, as explained in the Application of Self-Regulatory Principles to the Mobile Environment (Mobile Guidance), when allowing the third-party

---

<sup>1</sup> The DAA Principles consist of a suite of four documents: the Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles), the Self-Regulatory Principles for Multi-Site Data (MSD Principles), the Application of Self-Regulatory Principles to the Mobile Environment (Mobile Guidance) and the Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices (Cross-Device Guidance) (collectively, the Principles), *available at* <http://www.aboutads.info/principles>.

<sup>2</sup> The DAA Principles assign responsibilities to entities based on the role these entities are playing in a particular situation. Thus, an entity can be a first party, third party or service provider depending on the function it is performing. In the context of mobile applications, the first party is defined as the entity that owns or exercises control over the app, or its affiliates. Our references to “publishers” or “app publishers” in this case denote first parties under the Mobile Guidance. *See Mobile Guidance* Definition G at 7.

collection and use of data for cross-app<sup>3</sup> IBA, the application must provide notice and enhanced notice of this fact. Mobile app publishers that authorize the collection of precise location data<sup>4</sup> for IBA must also provide notice, enhanced notice, and a consent mechanism to their consumers. Publishers that collect personal directory data or personal information (PI) in the form of social security numbers or medical records information must obtain consent from their users before using this information for IBA.<sup>5</sup>

## COMPANY STATUS

iTriage LLC<sup>6</sup> (iTriage) is the publisher of the eponymous mobile application iTriage (iTriage App), which allows users to research health care information and manage health care options. The company is a wholly-owned subsidiary of Aetna Inc. (Aetna), a health care provider.<sup>7</sup> iTriage has been used by over 15,000,000 people as a symptom checker, doctor finder, or as a medical reference tool.<sup>8</sup>

## INQUIRY

This case arises from the Accountability Program's enforcement of the Mobile Guidance. In September 2015, the Accountability Program began a review of mobile apps on the iOS and Android operating systems for compliance with the DAA Principles. Selected apps included health care management applications. While testing these apps, the Accountability Program found that iTriage allowed third parties to collect user data for IBA without providing the required notice and enhanced notice. This data included IFA data, a unique, persistent identifier associated with each device that is generally used for IBA.<sup>9</sup> This prompted a full review of iTriage's compliance with the DAA Principles, including its app and its website.

---

<sup>3</sup> *Mobile Guidance* Definition D at 5. ("Cross-App Data is data collected from a particular device regarding application use over time and across non-Affiliate applications. Cross-App Data does not include Precise Location Data or Personal Directory Data.")

<sup>4</sup> *Mobile Guidance* Definition K at 9. ("Precise Location Data is data obtained from a device about the physical location of the device that is sufficiently precise to locate a specific individual or device.")

<sup>5</sup> See *OBA Principles* § VI at 16-17; *Mobile Guidance* § VIII at 32. Consent, as defined in the OBA Principles and Mobile Guidance, is an action in response to a "clear, meaningful, and prominent notice" regarding collection practices. *OBA Principles*, Definition D at 10. See also *Mobile Guidance* Definition B at 4.

<sup>6</sup> iTriage, <https://www.itriagehealth.com> (last visited May 13, 2016), see also iTriage, <http://www.itriagehq.com/> (last visited May 13, 2016).

<sup>7</sup> Aetna, <https://www.aetna.com/> (last visited May 13, 2016).

<sup>8</sup> See, e.g., PC World, *iTriage for Android*, <http://www.pcworld.com/product/453000/itriage-mobile-health.html> (last visited June 10, 2016).

<sup>9</sup> Utilizing the Accountability Program's testing equipment, we were able to capture and inspect Internet Protocol (IP) packets being transmitted from the app. Through analysis of the app's network traffic, we observed third parties known to engage in IBA collecting data through the app. Specifically, the Accountability Program noted the collection of Android's Advertising ID (AAID or IFA), a unique alphanumeric string used to identify a particular device for advertising purposes. AAIDs are the Android equivalent of Apple's Identifiers for Advertisers (IDFA). See Greg Sterling, *Google Replacing "Android ID" with "Advertising ID" Similar to Apple's IDFA*, Marketing Land (October 31, 2013), <http://marketingland.com/google-replacing-android-id-with-advertising-id-similar-to-apples-idfa-63636>; see also Grace Fletcher, *The Impact of iOS 7 on Mobile Attribution*, Tune.com blog (August 27, 2013), <http://www.tune.com/blog/impact-ios-7-mobile-attribution/>; see also DoubleClick, *Target Mobile Apps With IDFA or AAID*, DoubleClick Ad Exchange Buyer Help, <https://support.google.com/adxbuyer/answer/3221407?hl=en> (last visited Apr. 20, 2016). See also *Mobile Guidance* Definition D at 5. ("Cross-App Data is data collected from a particular device regarding application use over time

We first examined the iTriage App's pages in both Apple and Google's mobile application stores for the presence of enhanced notice links, which are required when third parties collect cross-app data through an application for use in IBA. The Accountability Program could only locate a link to a privacy policy for the iTriage App on the application's page in the Google Play Store. Clicking on the link took us to the top of the privacy policy for the iTriage App and website, as opposed to directing us to a section describing third-party IBA taking place through the mobile app. However, the information provided in the discussion of third-party advertising was limited to an explanation of cookies, with no mention of the other kinds of identifiers such as IFAs used in mobile apps. Moreover, iTriage did not provide opt-out instructions.<sup>10</sup> Furthermore, the Accountability Program could not locate a link to the privacy policy or any other IBA disclosure on the iTriage App page in the Apple App Store, as required by the Mobile Guidance.

The Accountability Program then investigated whether iTriage satisfied the enhanced notice requirements through alternative means. During testing on both Android and Apple devices, the Accountability Program could not find links to an IBA disclosure either during download or upon first opening the app, which are the alternative times at which enhanced notice may be provided when it is not provided through a link in the App Stores. The Accountability Program noted that the app prompted the user to assent to its terms of use prior to beginning use, but this notice did not include a discussion of IBA or an opt-out, and no choice mechanism was provided. Moreover, the Accountability Program could not locate a statement indicating adherence to the DAA Principles in the privacy policy or elsewhere on the application or website.

During testing of the app, the Accountability Program noted that immediately prior to download, the iTriage App requested through permission tools that the user grant the application access to the user's identity, calendar, location, photo and media files, and Wi-Fi connection information.<sup>11</sup> The permission tools were silent as to any transfer of this information to third parties or whether this information would be used for IBA. After downloading the iTriage App, the Accountability Program noted that the application prompted the user to accept its terms and conditions prior to beginning use.

---

and across non-Affiliate applications. Cross-App Data does not include Precise Location Data or Personal Directory Data.”)

<sup>10</sup> iTriage, *Privacy Policy*, [https://www.itriagehealth.com/legal/privacy\\_policy](https://www.itriagehealth.com/legal/privacy_policy) (August 7, 2014). (“THIRD PARTY ADVERTISING We may use third-party advertising companies to serve ads when you visit the Applications. Please note that these companies may use information about your use of the applications to provide advertisements about goods and services that may be of interest to you. In the course of serving advertisements to the applications, these companies may place or recognize a unique cookie on your browser. If you would like more information about this practice, and to know your choices about not having this information used by these companies, please visit [http://networkadvertising.org/optout\\_nonppii.asp](http://networkadvertising.org/optout_nonppii.asp).”) The Accountability Program notes that the discussion of how third party advertising works focuses only on cookies and is therefore not completely accurate. Browser cookies are mainly used in advertising for the collection of data from websites and the delivery of advertisements on a particular web page. A user might reasonably think, based on this discussion that by clearing her cookies, or using a browser-based opt out tool, her information would no longer be collected and used for IBA. Applications rely on different unique identifiers that can operate in an application system, generally an IDFA, for the service of ads. We found that the app did, in fact, collect the testing device's IDFA.

<sup>11</sup> The Accountability Program noted during testing on an Apple device that the app asked for permission to access location following download and prior to accepting the terms of use of the app.

After download, the iTriage App gave the user an option of creating a new account, logging into an existing account, or proceeding with use of the app without an account. The Accountability Program noted that the iTriage App allowed users to create an account that includes the last four digits of their social security number, their date of birth, their address, and information about their health insurance carrier. A user could also add information to their account about their health insurance, health care providers, appointments, medical conditions, procedures, and medication. It was not clear whether that information would be used or shared with third parties for IBA. When the Accountability Program tried to create an account, it did not receive notice as to how information in that account could be used or transferred to a third party. Moreover, it was unclear from the privacy policy whether iTriage was using PI for IBA, as the privacy policy indicated that the application and its third-party service providers may collect PI, including “social security number”<sup>12</sup> and that PI could be used to present offers and products tailored to a user.<sup>13</sup>

Looking further, the Accountability Program noted that users who do not create an account may still interact with a number of the iTriage App’s features, including search functions for symptoms, doctors, medical facilities, conditions, medications, and procedures. The app also features a list of medical hotlines, a spotlight feature that provides summaries of some of iTriage’s tools and general health tips, a news feature which provides articles on medical topics, a survey link that directs users to a survey which asks them questions about how they organize their health information, and an education link that directs users to [www.healthathand.com](http://www.healthathand.com). While the Accountability Program noted in the iTriage privacy policy that “third-party advertising companies... may use information about your use of the Applications to provide advertisements about goods and services that may be of interest to you”<sup>14</sup> it was not clear from the privacy policy whether sensitive health information that the user provides to utilize the app’s functions would be used for IBA.

The Accountability Program also noted in iTriage’s privacy policy that iTriage stated that it may share location data with its “marketing partners to enable them to provide [the user] with more personalized content.”<sup>15</sup> It was not clear from this description whether iTriage was collecting and sharing precise location data for IBA purposes.

---

<sup>12</sup> iTriage, *Privacy Policy* (August 7, 2014), [https://www.itriagehealth.com/legal/privacy\\_policy](https://www.itriagehealth.com/legal/privacy_policy). (August 7, 2014). (““Personal Information” is information that identifies you as an individual. We and our service providers may collect Personal Information from you, such as: ● Name, ● Postal address (including billing and shipping addresses) ● Telephone number, ● E-mail address ● Credit and debit card number ● Social Security number [sic] Protected Health Information, Additional Health Information and Other Information, as defined below, may be collected in connection with the Applications in addition to Personal Information.”)

<sup>13</sup> iTriage, *Privacy Policy*. (“How We May Use Personal Information We and our third-party service providers may use Personal Information:... To personalize your experience on the Applications by presenting products and offers tailored to you....”)

<sup>14</sup> iTriage, *Privacy Policy*. (“THIRD PARTY ADVERTISERS We may use third-party advertising companies to serve ads when you visit the Applications. Please note that these companies may use information about your use of the Applications to provide advertisements about goods and services that may be of interest to you. In the course of serving advertisements to the Applications, these companies may place or recognize a unique cookie on your browser.”)

<sup>15</sup> iTriage, *Privacy Policy* (August 7, 2014), [https://www.itriagehealth.com/legal/privacy\\_policy](https://www.itriagehealth.com/legal/privacy_policy). (“We may collect the physical location of your device, for example, using satellite, cell phone tower or WiFi signals... We may also share your device’s physical location, combined with information about what advertisements you viewed and other

We then examined iTriage’s website for compliance with the OBA Principles. The site allowed third parties known to engage in IBA to collect visitors’ data, but did not provide the enhanced notice link required by the OBA Principles.

Following its review, the Accountability Program sent an inquiry letter to iTriage detailing these issues in order to bring the company into compliance with the DAA Principles.

## COMPANY’S POSITION

Once the Accountability Program overcame some initial difficulty establishing a line of communication to iTriage and explained the DAA Principles, iTriage demonstrated a clear commitment to coming into compliance. It immediately began an internal compliance review.

In response to the Accountability Program’s inquiry, iTriage acknowledged the problems that had been discovered during the compliance review and indicated that, as a result, it had swiftly begun to address the concerns raised by the inquiry. Both in forming and executing its compliance plan, iTriage worked diligently with the Accountability Program to modify its application and website in order to reach full compliance. Aetna, the parent company of iTriage, stated that it was not presently engaged in IBA but also acknowledged that it would be beginning IBA campaigns on its websites in the near future. In the course of consulting with the Accountability Program, Aetna committed to taking prophylactic steps to ensure that its website would be compliant with DAA Principles before it begins authorizing companies to engage in IBA on its website.

After some probing by the Accountability Program to learn what types of user data third parties were allowed to collect for IBA and a thorough internal review by iTriage’s compliance and marketing teams, the company was able to confirm that it restricted its collection and use of data for IBA to the **way** consumers used the iTriage App’s functions and did not allow any health data or personal information to be collected and used by third parties for interest segments. The information about consumers’ use of the many tools and features in the app was used to group them into segments based on the types of features and tools they were accessing and using so that they would be shown ads about the app on non-affiliate sites based on features and tools likely to spur their interest in further and fuller use of the app.

In order to meet their obligations in both the mobile and desktop environments, iTriage and Aetna committed to making the following changes:

### I. Mobile Guidance issues

---

information we collect, with our marketing partners to enable them to provide you with more personalized content and to study the effectiveness of advertising campaigns. We may also share deidentified information about your device's physical location for any purpose not prohibited by applicable law. In some instances, you may be permitted to allow or deny such uses and/or sharing of your device's location, but if you choose to deny such uses and/or sharing, we and/or our marketing partners may not be able to provide you with the applicable personalized services and content.”)

## 1. Cross-app enhanced notice

To address its cross-app enhanced notice obligations under the Mobile Guidance, iTriage committed to adding a link entitled “Interest Based Ads” to its pages in the Google Play and Apple App Stores, and to the iTriage application. These links will direct to an IBA disclosure which will include a link to the DAA opt-out page at [www.aboutads.info/choices](http://www.aboutads.info/choices) and a link to the AppChoices app at [www.aboutads.info/AppChoices](http://www.aboutads.info/AppChoices) where users can find the AppChoices app for download and a statement of adherence to the DAA Principles.

## 2. Sensitive Data Principle

As stated above, after conducting a review of the types of information that its app collects, iTriage confirmed that no sensitive categories of information as defined in the DAA Principles were collected by third parties for IBA.<sup>16</sup> Therefore, there was no compliance issue with respect to the collection and use of sensitive data.

## 3. Precise Location Data

iTriage’s review of its practices revealed that it authorizes third-party companies to collect precise location data from the iTriage App. To come into compliance with the Mobile Guidance, iTriage committed to replacing the existing precise location data feed that third parties access with a new data feed which will only authorize the third-party collection of coarse location data. The Accountability Program found that this commitment resolved the issue of notice and choice regarding the collection precise location data by third parties.

## 4. Personal Directory Data

After discussions with the Accountability Program and an internal examination of its practices, iTriage determined that personal directory data was not used for IBA.

## II. OBA Principles

### 1. First Party enhanced notice

#### i. iTriage website

To come into compliance with the OBA Principles, iTriage committed to adding a link entitled “Interest Based Ads” to the footer of its website on each page where data for IBA is collected by third parties. The link will direct users to an IBA disclosure which will describe the third-party data collection on the iTriage website. The disclosure will include a link to the DAA’s [www.aboutads.info/choices](http://www.aboutads.info/choices) opt-out page and a statement of adherence to the DAA Principles

---

<sup>16</sup> Under §VI.B. of the OBA Principles and §VIII. of the Mobile Guidance, Health and Financial Data includes financial account numbers, pharmaceutical prescriptions, social security numbers, or medical records about a specific individual. Under Definitions H of the OBA Principles and J of the Mobile Guidance, Personal Identifiable Information is information about a specific individual including address, names, telephone number, and email address when used to identify a particular individual. *OBA Principles* at 11, 17. *See also Mobile Guidance* at 9, 32.

ii. Aetna website

After conducting a full investigation of Aetna and its affiliates' IBA practices, Aetna found that there are no current active IBA campaigns on Aetna websites. However, the company noted that there are imminent plans to launch IBA on its websites and committed to ensuring that its new IBA practices will be compliant with the DAA Principles. Aetna pledged to add a compliant enhanced notice link to all Aetna webpages that will allow third-party data collection for IBA. This compliant enhanced notice link will direct visitors to an IBA disclosure that will contain a link to the DAA's opt-out page and a statement of adherence to the DAA Principles.

## DECISION

The Mobile Guidance adapts the desktop-oriented rules of the OBA Principles to the mobile world, including the core requirements to provide transparency and consumer control of IBA. In particular, when first parties permit third parties to collect data through their apps for use in IBA, they must provide enhanced notice and choice about such third-party data collection for IBA.<sup>17</sup>

### I. Mobile Guidance issues

#### 1. First party enhanced notice and consumer control for cross-app data collection

Since iTriage authorizes third parties to engage in cross-app IBA through its mobile app, it has "first party"<sup>18</sup> obligations under the Mobile Guidance.

According to section III.A.(3) of the Mobile Guidance, first parties who affirmatively authorize a third party to collect or use cross-app data for IBA must provide a clear, meaningful, and prominent link to a disclosure that 1) describes the third party collection, 2) points to a choice mechanism/setting or lists all third parties with links to their opt outs, **and** 3) contains a statement of adherence to the DAA Principles.<sup>19</sup> The enhanced notice link must be provided prior to download (e.g., in the app store on the application's page), during download, on first opening of the app, **or** at the time cross-app data is first collected, **and** in the application's settings or any privacy policy.<sup>20</sup>

---

<sup>17</sup> *Mobile Guidance* at 17.

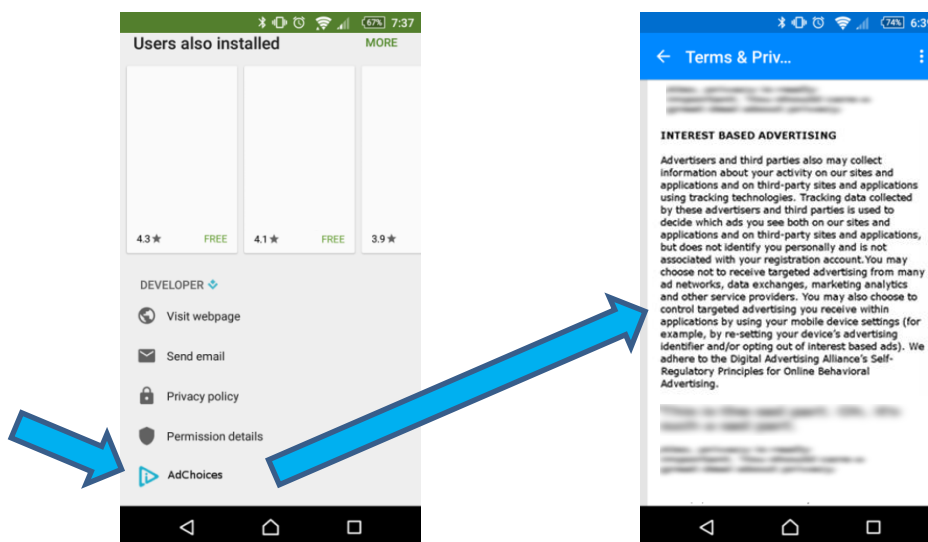
<sup>18</sup> *Mobile Guidance* Definition G at 7. ("A First Party is the entity that is the owner of an application, or has Control over the application, with which the consumer interacts, and its Affiliates.")

<sup>19</sup> *Mobile Guidance* at 17.

<sup>20</sup> *Mobile Guidance* at 17. We note that where the third party is unable to provide enhanced notice and choice in an app, the first party should work with the third party to ensure that such notice and choice are provided. *See Mobile Guidance* § III.B.(1) at 18-19. *Compare* Online Interest-Based Advertising Accountability Program, *Compliance Warning*, available at <http://www.asrcreviews.org/wp-content/uploads/2013/10/Accountability-Program-First-Party-Enhanced-Notice-Compliance-Warning-CW-01-2013.pdf> at 2. ("Both the third party and the first party share responsibility for provision of enhanced notice. Because the third party which is collecting the data generally has no direct means to provide notice and choice on the website where its data collection is occurring, providing just-in-time notice of collection and an opt out requires cooperation between the third party engaged in the collection and the first party on whose website such collection is permitted.")

These enhanced notice requirements make information about privacy more accessible to users, so they can make an informed decision about whether to participate in data collection and use for IBA. The enhanced notice link must go **directly** to the place where the app explains its IBA practices. Moreover, the link must be provided **at or before** the moment a user's engagement with the app results in third-party data collection for IBA. This replaces the old-fashioned practice of burying information about IBA—if it was provided at all—somewhere in the privacy policy for the consumer to unearth. It also requires that the company's disclosure explain to consumers how they can opt out of IBA, including providing links to easy-to-use opt-out mechanisms like the DAA's AppChoices tool.

Since the Mobile Guidance is new, we provide an example of enhanced notice below, by way of illustration of one of the many compliant ways of providing enhanced notice in the mobile world. As discussed, application publishers may use a privacy policy link in the application store as enhanced notice so long as it leads to the **relevant section** of the privacy policy.



To achieve full compliance, iTriage committed to providing enhanced notice links in its pages under the Google Play and Apple App Store. These links will direct users to an IBA disclosure page that includes an opt-out mechanism and a statement of adherence to the DAA principles.

## 2. Requirements under the Sensitive Data Principle

The Mobile Guidance triggers additional responsibilities when companies authorize the collection of certain types of data. The Mobile Guidance also incorporates all of the self-regulatory principles and definitions of the OBA Principles, including the heightened requirements of section VI., the Sensitive Data Principle.<sup>21</sup>

Under section VI.B. of the OBA Principles and section VIII. of the Mobile Guidance, companies may not collect sensitive data, including social security numbers, pharmaceutical prescriptions,

<sup>21</sup> *Mobile Guidance* Overview at 1, § VIII. at 32. See also OBA Principles § VI. at 16-17.



or medical records for IBA without notice and prior consent.<sup>22</sup> Consent is defined as an affirmative action taken by the consumer in response to a clear notice that explains what information is being collected, whether it will be transferred and how it will be used for IBA.<sup>23</sup>

Following discussions with the Accountability Program and an internal investigation, iTriage confirmed that it did not collect sensitive categories of information covered by section VI.B of the OBA Principles or section VIII. of the Mobile Guidance for IBA. The Accountability Program therefore determined that there was no compliance issue related to the collection of sensitive data for IBA.

### 3. Precise Location Data

According to section IV.A.(1) of the Mobile Guidance, first parties must provide clear, meaningful, and prominent notice when they affirmatively authorize third parties to collect precise location data for use in IBA from or through their app(s).<sup>24</sup> This notice must be placed on the company's website or be accessible through its app(s) and provide clear descriptions of: 1) the fact that precise location data is transferred to or collected by any third party, 2) instructions for accessing and using a tool for providing or withdrawing consent, 3) **and** the fact that the first party adheres to the DAA Principles.<sup>25</sup>

In addition to a general notice requirement under section IV.A.(1) of the Mobile Guidance, first parties must also provide enhanced notice under section IV.A.(3). This enhanced notice must be a clear, meaningful, and prominent notice of the fact that the first party transfers or authorizes third party collection of precise location data.<sup>26</sup> The first party must also provide a link within the enhanced notice to the disclosure required under section IV.A.(1) of the Mobile Guidance.<sup>27</sup> This notice and link must be provided either during the process of downloading the app, at the time the app is opened, **or** at the time such data is first collected **and** in the app's settings or any privacy policy.<sup>28</sup> Companies may use the mechanisms provided by the app store to fulfill this notice requirement.<sup>29</sup> A company may also supply its own method of enhanced notice as long as it is as clear, meaningful, and prominent as the notice required by section IV.A.(3) of the Mobile Guidance.<sup>30</sup>

---

<sup>22</sup> *OBA Principles* at 16-17, *Mobile Guidance* at 32. Consent, as defined in the OBA Principles and Mobile Guidance, is an action in response to a "clear, meaningful, and prominent notice" regarding collection practices. *See also OBA Principles* Definition D at 10. *See also Mobile Guidance* Definition B at 4.

<sup>23</sup> *OBA Principles* at 10, *see also Mobile Guidance* at 4.

<sup>24</sup> *Mobile Guidance* at 21.

<sup>25</sup> *Mobile Guidance* at 21-22.

<sup>26</sup> *Mobile Guidance* at 23-24.

<sup>27</sup> *Mobile Guidance* at 24.

<sup>28</sup> *Mobile Guidance* at 24. ("A First Party can satisfy the requirement to provide download notice under section IV.A.(3)a by participating in a notice mechanism that satisfies this Principle and is offered by an application platform or an application market provider that makes the application available for download.")

<sup>29</sup> *Id.* at 24-25. We note that in order to be compliant, the app store notice must meet the requirements of the Mobile Guidance, including notice of transfer to third parties.

<sup>30</sup> *Mobile Guidance* at 23.

Further, under section IV.B.(1), first parties should obtain consent to allow third parties to collect precise location data for IBA purposes prior to collection.<sup>31</sup> This consent tool should be easy-to-use and should apply to the app and device from which the consent is provided.<sup>32</sup> The first party is also required to provide an easy-to-use tool for withdrawing consent at any time.<sup>33</sup> Consent, as described in the Mobile Guidance, is an action in response to a “clear, meaningful, and prominent notice.”<sup>34</sup> A company can satisfy this principle by allowing consumers to provide or withdraw consent as a part of the process of downloading and installing an app or through an app’s settings.<sup>35</sup> A company may also use permissions tools provided by an app platform or app market provider to satisfy this requirement.<sup>36</sup>

As discussed in the previous section, following consultation with the Accountability Program, iTriage decided to cease authorizing the collection of precise location data through its app by third parties and only allow the collection of coarse location data. The Accountability Program found that since there were no longer any existing IBA practices that triggered the precise location data requirements of the Mobile Guidance, this issue was resolved.

#### 4. Personal Directory Data

The collection and use of personal directory data for IBA has requirements commensurate with the sensitive nature of this type of data to many consumers. “Personal directory data” is defined by the Mobile Guidance as data created by the consumer on his or her device.<sup>37</sup> To the extent that a company collects personal directory data for use in IBA from a device, “the entity is a third party.”<sup>38</sup> With respect to personal directory data, only the entity that provides the location where the personal directory data is stored is considered a “first party.” Under section V. of the Mobile Guidance, the app may not access personal directory data for IBA without prior authorization from the first party, which in this case, is the device/operating system on which that data is stored.<sup>39</sup> In addition to permission from the device, prior affirmative consent must be obtained from the consumer prior to accessing personal directory data for IBA.<sup>40</sup> Moreover, consumer consent must be obtained before transferring personal directory data to another entity for IBA.<sup>41</sup>

As discussed in the previous section, following the Accountability Program inquiry, iTriage confirmed that it did not utilize personal directory data for IBA. The Accountability Program found that since there were no existing IBA practices that triggered the Mobile Guidance’s personal directory data obligations, this issue was resolved.

---

<sup>31</sup> *Mobile Guidance* at 25-26.

<sup>32</sup> *Mobile Guidance* at 25-26

<sup>33</sup> *Mobile Guidance* at 26.

<sup>34</sup> *Mobile Guidance* Definition B at 4.

<sup>35</sup> *Mobile Guidance* at 27. We note the app’s settings may only be used by the first party if they satisfy the actual requirement, *e.g.*, provide notice of transfer of location data to a third party for IBA.

<sup>36</sup> *Id.*

<sup>37</sup> *Mobile Guidance* Definition I at 8. (“Personal Directory Data is calendar, address book, phone/text log, or photo/video data created by a consumer that is stored on or accessed through a particular device.”)

<sup>38</sup> *Mobile Guidance* Definition N at 12.

<sup>39</sup> *Mobile Guidance* at 30.

<sup>40</sup> *Mobile Guidance* at 30.

<sup>41</sup> *Mobile Guidance* at 30.

## II. OBA Principles issues

In the course of its investigation, the Accountability Program discovered compliance issues with the iTriage website under the OBA Principles. iTriage's obligations as a first-party<sup>42</sup> website operator are discussed below.

### 1. First party enhanced notice link requirements

Under section II.B. of the OBA Principles, when a first party allows non-affiliates<sup>43</sup> to collect or use data for IBA on its own website, it must ensure that an enhanced notice link appears on every page where this collection or use occurs.<sup>44</sup> This link must direct consumers to a disclosure of non-affiliate IBA activity occurring on the website.<sup>45</sup> This disclosure must provide a link to an easy-to-use opt-out mechanism as well as a statement of adherence to the DAA Principles.<sup>46</sup>

#### i. iTriage website

iTriage committed to adding an enhanced notice link on each page of its website which allow third-party data collection for IBA. This enhanced notice link, entitled "Interest Based Ads," will direct users to an IBA disclosure that includes a link to the DAA's [www.aboutads.info/choices](http://www.aboutads.info/choices) page.

#### ii. Aetna website

To prepare for new IBA campaigns on the Aetna website, Aetna pledged to add an enhanced notice link on each of its webpages where third-party entities collect data for IBA. The link will direct users to an IBA disclosure which will include a link to the DAA's opt-out page.

## CONCLUSION

Since the Accountability Program began mobile enforcement in September 2015, companies have been put on notice that they must implement notice and choice for the third-party collection of cross-app data and precise location data, and follow the requirements of the Children's Online Privacy Protection Act of 1998 (COPPA) when authorizing IBA on child-directed apps. This case represents a continuation of the Accountability Program's enforcement efforts, and reminds companies that consent for the use in IBA of user-generated data, or personal directory data, falls under the purview of the DAA Principles. Moreover, companies must obtain consent from users before using in IBA sensitive data such as social security numbers, medical records, or pharmaceutical information.

---

<sup>42</sup> *OBA Principles* Definition Fat 10. ("A First Party is the entity that is the owner of the Web site or has Control over the Web site with which the consumer interacts and its Affiliates.")

<sup>43</sup> *OBA Principles* Definition J at 11. ("An entity is a Third Party to the extent that it engages in Online Behavioral Advertising on a non-Affiliate's Web site.")

<sup>44</sup> *OBA Principles* at 13-14.

<sup>45</sup> *Id.*

<sup>46</sup> *OBA Principles* § II.B. at 13-14. First parties may either link to an industry-developed opt-out website (e.g., <http://aboutads.info/choices>) or list each third party engaged in IBA on its website and provide links to each company's opt-out tool.

As the mobile economy continues to expand, apps provide services that include entertainment, shopping, navigation, education, and health care. The Accountability Program's mobile enforcement began with a sweep of popular gaming and entertainment apps featured in the App Stores. Our enforcement efforts have now expanded to include inquiries into healthcare related apps. The Accountability Program will continue to investigate applications that provide services in various categories.

Self-regulation requires support from all actors that participate in data collection for IBA, from small mobile app publishers trying to monetize their applications to the largest companies. It is especially critical that companies that have access to data that may be sensitive, as set forth in the OBA Principles and the Mobile Guidance, be scrupulous in ensuring that they are fully transparent about and give consumers' an easy-to-use choice mechanism, prior to the collection and use of such information for IBA.

The Accountability Program appreciates the willingness of iTriage to participate in its formal review process and come into full compliance with the Mobile Guidance and OBA Principles. While iTriage is not currently allowing any third party to draw on any healthcare related information on its app, it is mindful of the potential sensitivity such use might pose. The company has assured the Accountability Program that it will be fully transparent if it allows third parties access to such information for IBA and will follow the appropriate consent requirements under the OBA Principles that apply to such third-party collection and use. Both iTriage and its parent company, Aetna, are taking prophylactic steps, including those set out in this decision, to provide transparency and consumer control on the iTriage App and the Aetna website before undertaking any IBA campaigns that expand the types of data collected and used by third parties. As is customary, the Accountability Program will retain jurisdiction until iTriage and Aetna have fully executed the updates that are now underway. In light of the exemplary way that iTriage and Aetna have responded to our inquiry, we are confident that they will continue to make these changes to come into full compliance as quickly as possible.

## **COMPANY'S STATEMENT**

iTriage and Aetna are committed to treating user information with care and respect and managing our websites and mobile applications in a manner that is compliant with law. We share the Accountability Program's commitment to transparency and consumer control, and it is our intent at all times to provide both elements to consumers. We appreciate the opportunity to work with the Accountability Program to further strengthen our efforts to promote transparency and align our advertising initiatives with the highest standards of industry best practices.

## **DISPOSITION OF DECISION**

Practices voluntarily corrected; jurisdiction retained while company completes updates.



**Genie Barton**  
**Vice President and Director**  
**Online Interest-Based Advertising Accountability Program**